IT IS CLAIMED:

1. A system for use in distributing authentication information to users of remote devices, comprising:

an authentication information store configured to store authentication information for a plurality of users;

an authentication system configured to receive a request for authentication information for one of the plurality of users from a remote device;

wherein the request includes identity information for use in determining whether the request is from one of the plurality of users,

wherein the authentication system retrieves based on the identity information the authentication information for the one of the plurality of users from the authentication information store;

wherein the retrieved authentication information is provided to the remote device.

2. The system of claim 1, wherein the authentication information is to be used in a two-factor authentication scheme.

3. The system of claim 1, wherein the authentication information store includes a seed store configured to store a plurality of seeds, wherein the authentication system is configured to receive a seed request, including an access code generated using one of the plurality of seeds, from the remote device, to retrieve the one of the plurality of seeds from the seed store, to calculate an access

code using the retrieved seed, to determine whether the calculated access code matches the received access code, and to return the retrieved seed to the remote device where the calculated access code matches the received access code.

4. The system of claim 1, wherein the request comprises a Hypertext Transfer Protocol (HTTP) connection request.

5. The system of claim 1, wherein the request includes a network password and a digital signature, wherein the network password and digital signature are verified by the authentication system before the authentication information is provided to the remote device.

6. The system of claim 1, wherein the identity information includes user information and account information.

7. The system of claim 6, wherein the identity information identifies a particular user and corresponding authentication information being requested, and allows the authentication system to authenticate the user requesting the authentication information.

8. The system of claim 1, wherein the identity information in the request enables two-factor authentication at the computer network.

9. The system of claim 8, wherein the identity information includes a network password entered by

the user of the remote device and a digital signature generated based on a transformation of at least a portion of the information in the request, a signature key, and a signature algorithm.

10. The system of claim 1, wherein the authentication system does not provide the authentication information to the remote device because a match was not found in the authentication information store based upon the identity information.

11. The system of claim 1, wherein the authentication information includes a password which is normally not known to the user of a remote device but is required for remote access to resources in the computer network.

12. The system of claim 1, wherein the authentication information includes an access code which is normally not known to the user of a remote device but is required for remote access to resources in the computer network.

13. The system of claim 1, wherein the retrieved authentication information includes an expiring password which is valid for a relatively short period of time.

14. The system of claim 13, wherein the short period of time is on the order of minutes.

15. The system of claim 1, wherein the retrieved authentication information includes an expiring access code which is valid for a relatively short period of time.

16. The system of claim 1, wherein the retrieved authentication information includes a non-expiring password and is stored in a protected data store on the remote device.

17. The system of claim 1, wherein the retrieved authentication information includes a seed from which access codes are to be generated by the remote device, wherein the seed is stored in a protected data store on the remote device.

18. The system of claim 1, wherein the retrieved authentication information is for use by the remote device to gain access to a corporate local area network (LAN).

19. The system of claim 18, wherein two-factor authentication is used in the LAN to authenticate a user requesting remote access to the LAN, wherein the retrieved authentication information is used in performing two-factor authentication in order to gain access to the LAN.

20. The system of claim 19, wherein the retrieved authentication information includes a seed for use by the remote device's two-factor code generator to produce an access code, wherein the access code is also based upon a value provided by the remote device's clock, wherein the access code is used by the remote device to gain access to the LAN;

wherein the seed is used by the authentication system to also generate an access code for use in a comparison with the access code generated by the remote device;

wherein access to the LAN is granted based upon the comparison.

21. The system of claim 20, wherein the remote device only generates the access code when access to the LAN is requested by the user of the remote device.

22. The system of claim 20, wherein the authentication information store includes an index by user name that indicates users authorized for remote access to the LAN.

23. The system of claim 22, wherein the authentication information store stores user seed values for use in generating access codes.

24. The system of claim 1, wherein the remote device is a wireless mobile communication device.

25. The system of claim 24, wherein the remote device stores the authentication information in a data store.

26. The system of claim 25, wherein the data store is implemented in a smart card.

27. The system of claim 25, wherein the data store is implemented in a Universal Serial Bus (USB) token.

28. The system of claim 1, wherein the remote device is a desktop computer.

29. The system of claim 1, wherein the remote device communicates with the authentication system over a communication system, wherein the communication system includes a wide area network (WAN) and a wireless network gateway.

30. A method of distributing authentication information for remotely accessing computer resources, comprising the steps of:

receiving a request for the authentication information from a remote device, the request comprising identity information of a user of the remote device;

authenticating the user based on the identity information in the request; and

returning the authentication information to the remote device so that the remote device may access the computer resources based upon the returned authentication information.

31. An apparatus for use in handling authentication information for users of remote devices, comprising:

an authentication information store configured to store authentication information for a user of a remote device, the authentication information provided by a remote authentication system;

wherein a request from the remote device to the remote authentication system contains identity information;

wherein the authentication information is provided to the remote device after the request is processed based upon the identity information contained in the request;

a code generation system configured to retrieve the authentication information stored

in the authentication information store;

wherein access information is generated based upon the retrieved authentication information and is used in accessing a remote computer network.

32. A method for obtaining authentication information for use in remotely accessing a computer network, the method comprising the steps of:

providing a request from a user of a remote device to an authentication system for the authentication information;

wherein the request includes identity information for use by the authentication system to authenticate the user based on the identity information provided in the request;

receiving by the remote device the authentication information from the authentication system;

wherein the received authentication information is to be used by the remote device to access the computer network.